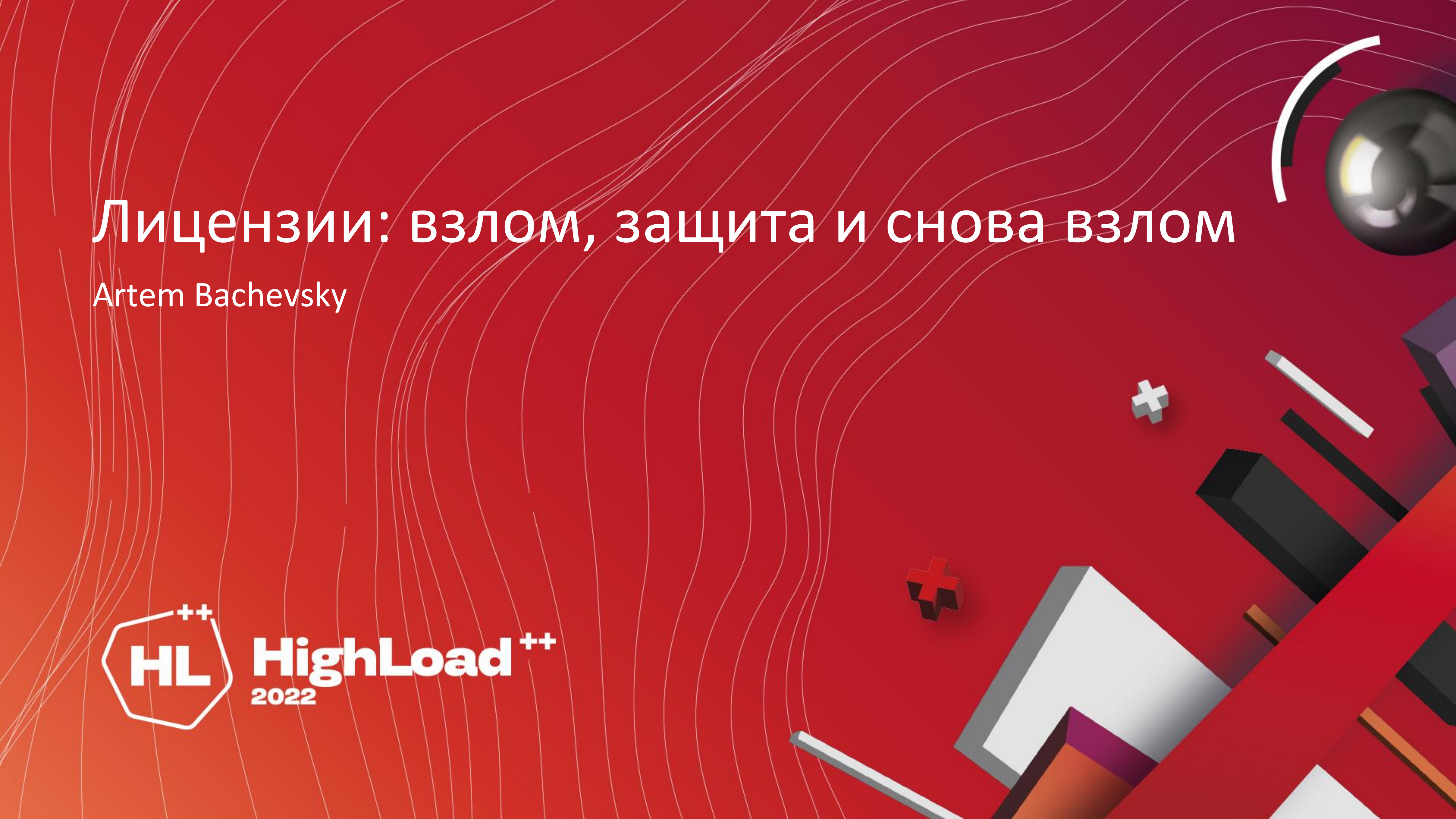


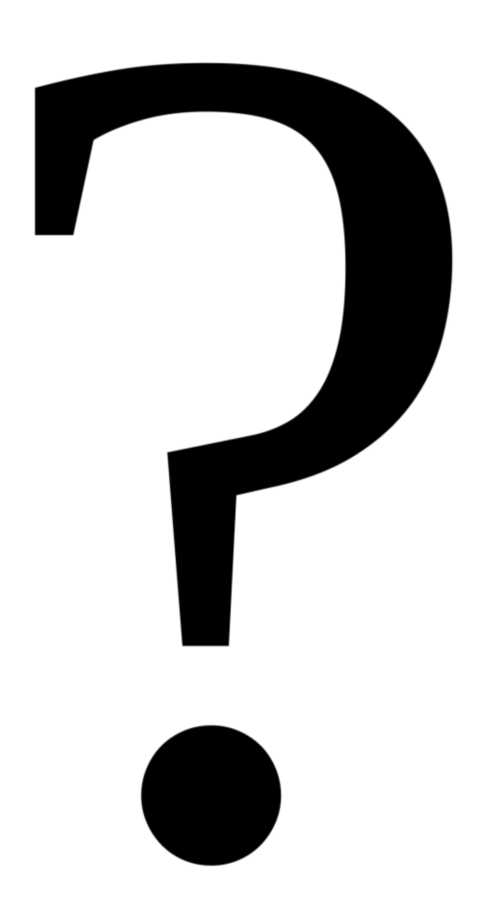
Лицензии: взлом, защита и снова взлом
Artem Bachevsky
HL
HighLoad++
2022

whoami

- Software developer -> AppSec Expert
- Пользователь лицензируемого софта
- Исследователь безопасности
- @frydaykg



О чем поговорим



- От чего, что и как защищаем?
- Как нас при этом ломают?
- И что мы можем противопоставить в ответ?



От чего?

- **Защита от несанкционированного использования программ** — система мер, направленных на противодействие нелегальному использованию программного обеспечения. При защите могут применяться организационные, юридические, **программные** и программно-аппаратные средства. (c) Wikipedia



Что?

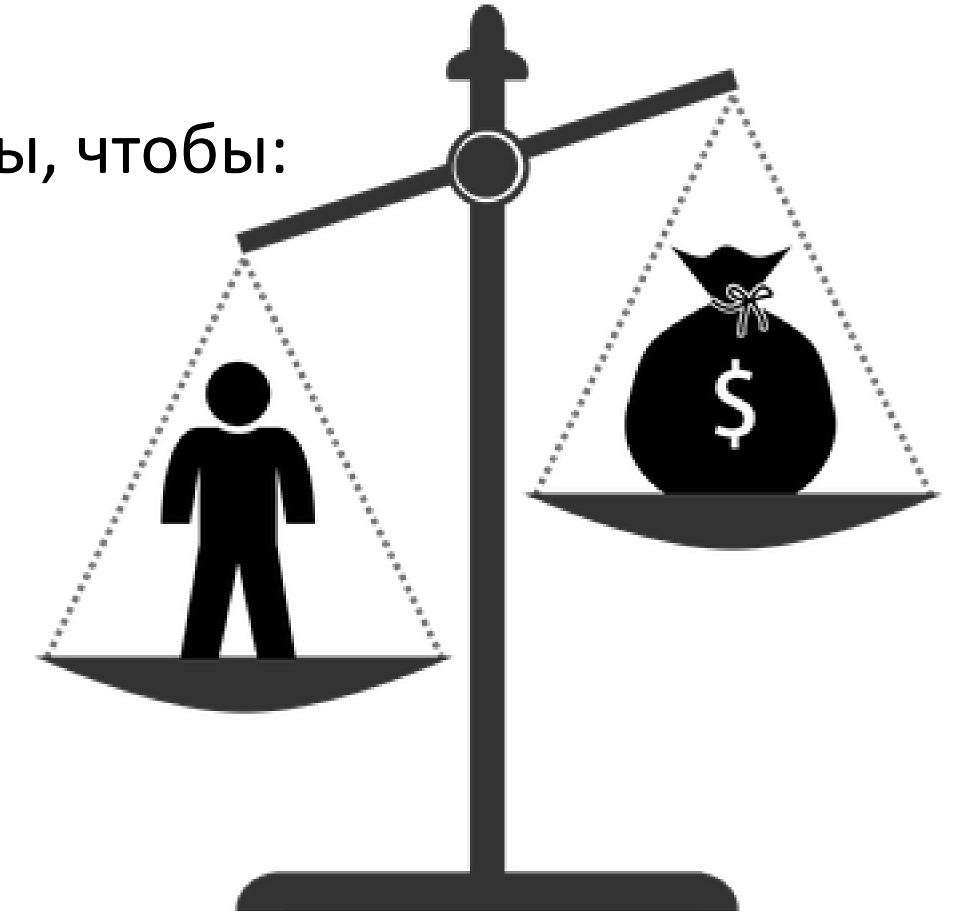
- Возможность использования ПО как такового
- Возможность использования ПО в оплаченные сроки
- Платный функционал
- Наши ограничения и лимиты



Основной принцип и задача

Подобрать такое соотношение мер защиты, чтобы:

- UX пользователя сильно не страдал
- Ломать защиту было дорого
- И очень хотелось бы заплатить…

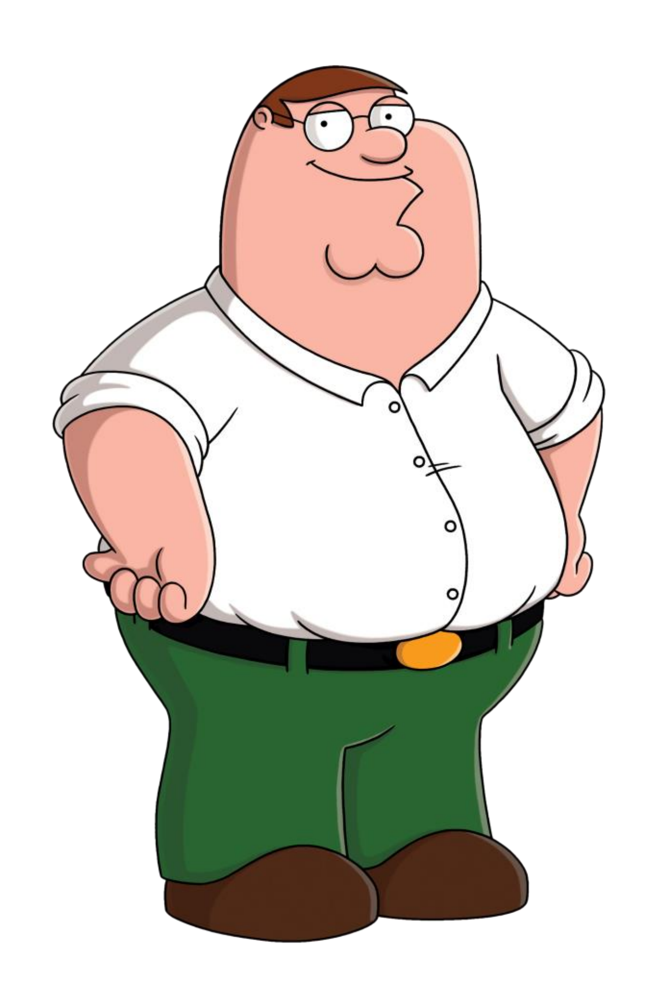




Активация ПО

По объекту:

- Толстый клиент
- Тонкий клиент (веб)





Активация ПО

По способу:

- Офлайн
- Онлайн
- Локальный сервер активации

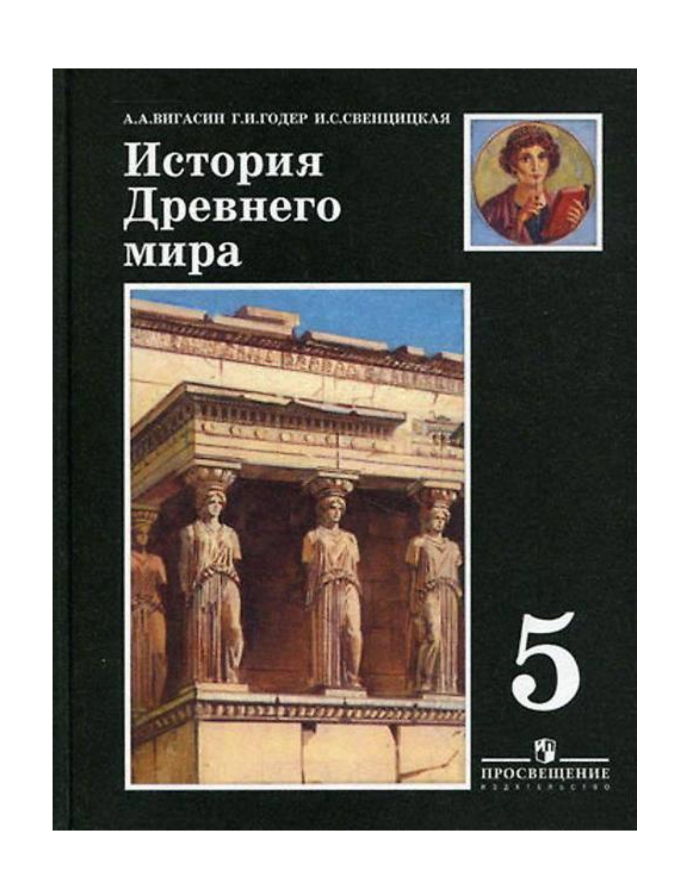


По способу активации: офлайн

Атаки

- Через распространение серийных ключей







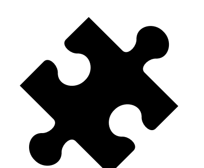
По способу активации: офлайн

Но если все же вам пришлось…

- Распространяйте уникальные инсталляторы
- Реализуйте систему телеметрии
- Поработайте с вашей EULA и организационными мероприятиями







Кейс: easy win





Кейс: easy win

- Активация есть!
- Активация принимает произвольный серийник!!

- Переход с CD на онлайн-модель дистрибуции



По способу активации: онлайн

Принцип

1. Генерируется отпечаток (fingerprint)
2. Попадает вендору
3. Вендор возвращает код активации
4. Код вводится в программу





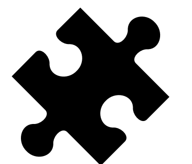
По способу активации: онлайн

Атаки

- Кейгены
- Патчинг
- Атаки на сервер активации
- Эмуляция среды





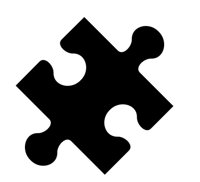


Кейс: атака на сервис активации

- Онлайн-активация
- Подписываем хэш от железа и делаем это лицензией
- Проверяем на возможность подмены железа

Что могло пойти не так?





Кейс: атака на сервис активации

Hacked by PhyRo

© файл в корне сервера проверки лицензии







Кейс: атака на сервис активации

Цепь только столь же сильна,

как ее самое слабое звено ©

Помните об:

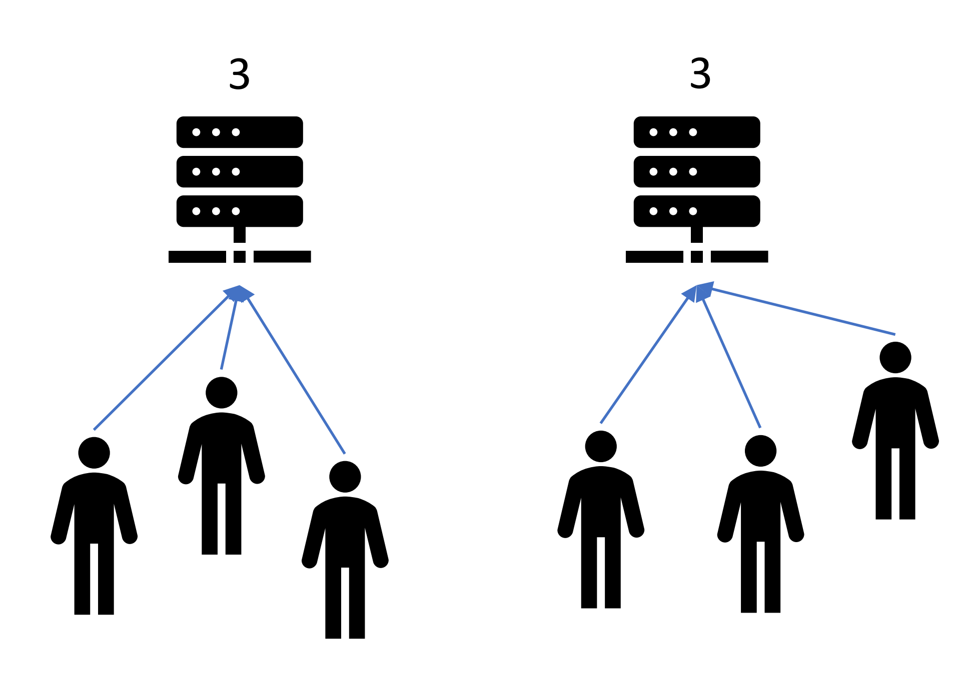
- Инфраструктуре
- Используемых сторонних компонентах



По способу активации: локальный сервер

Атаки

- Фейковый сервер
- Дублирование серверов активации



Инструменты

- Burp/Wireshark
- Декомпиляторы
- Прямые руки + nginx



Активация ПО

По объекту привязки:

- Уникальный инсталлятор
- Железу
- Профиль пользователя в ОС
- Учетная запись (прикладная)



Активация ПО: уникальный инсталлятор

Best case:

- Онлайн-активация
- Регулярная онлайн-проверка

В остальных случаях это будет фиаско, братан.

Зато появляется возможность трекинга распространения ПО!

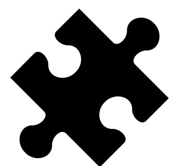


Активация ПО: железо

Принцип:

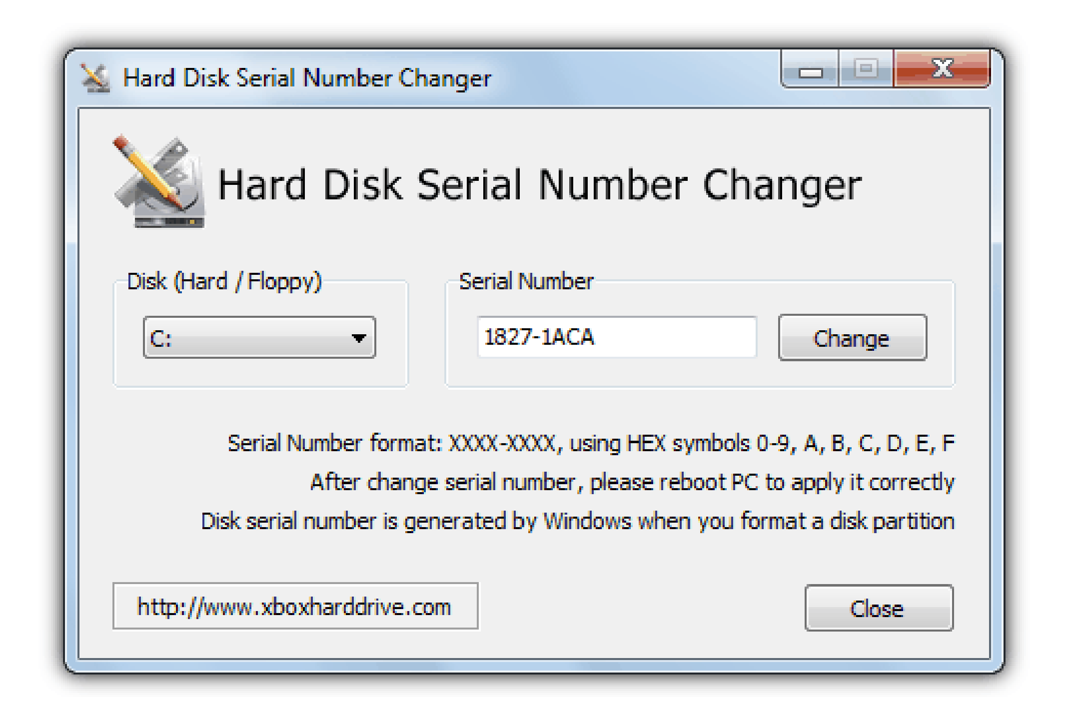
1. Собираем набор уникальных параметров железа
2. Хэшируем их
3. Вендор подписывает хэш
4. Подпись и есть лицензия
5. Софт периодически генерирует хэш и сравнивает его с подписью



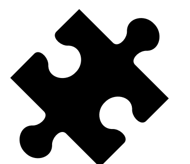
 Кейс: спуфинг железа

- Толстый клиент
- Привязка к железу
- Полуонлайн-активация
- На определенный период времени

Так, а что тут не так?







Кейс: спуфинг железа

- Слабые параметры железа
  - а есть ли сильные?
- Возможность запуска на виртуальных средах
  - Red Pill



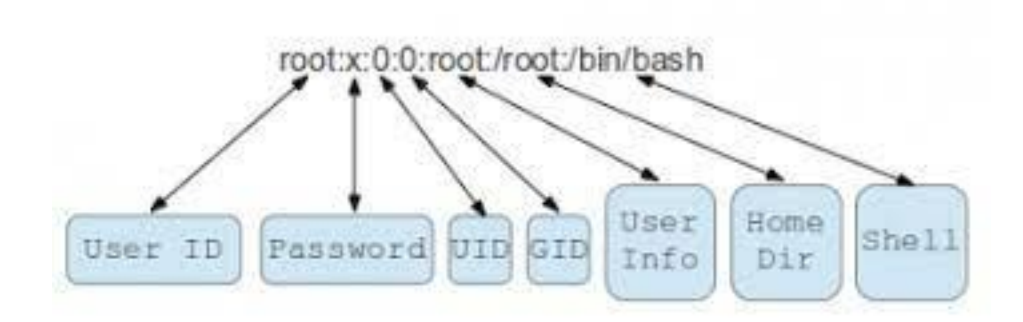




Активация ПО: профиль пользователя в ОС

Мы разрешаем пользоваться ПО только одному пользователю на лицензию, но при этом возможно на нескольких устройствах.

Объекты привязки: пользователь ОС, его метаданные





Активация ПО: профиль пользователя в ОС

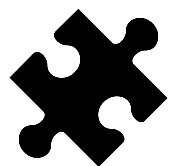
В реальности учитывается

- Количество запрошенных активаций на различные устройства за период
- Степень похожести пользовательских имен

Атаки

- Эмуляция среды исполнения (имя пользователя, перенос файлов лицензий)
- Фрод с количеством активаций на лицензию



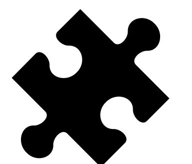


Кейс: перенос лицензий

- Популярная аппсек-тула
- Хранит лицензию в реестре или файле настроек

Как сломать?





Кейс: перенос лицензий

- Трекаем изменения файлов и реестра
  - Process monitor/strace
- Считаем diff до и после активации
- Выясняем точные метаданные для привязки
  - Глаза
  - Декомпиляторы
- Формируем патч на реестр, ОС, файловую систему
- PROFIT!!1



Активация ПО: прикладной пользователь

- Применимо для тонких клиентов
- Практически всегда решения с необходимостью доступа в Интернет
- Активация = факт захода в сервис с конкретным логином



Против лома нет приема

Если есть проверка – то ее всегда можно обойти.

Инструментарий:

- IDA Pro
- Ghydra
- Hopper
- Radare2
- ApkTool



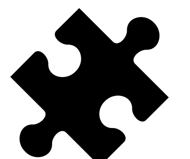


Кейс: бинарный патчинг

Наикрутейший вендор экшн-камер продает функцию для стабилизации видео



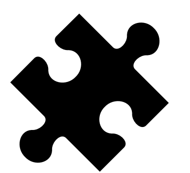




Кейс: бинарный патчинг

1. Анализ объекта
2. Декомпиляция
3. Патчинг





Кейс: бинарный патчинг

Инструменты в помощь

- file
- dotPeek
- .net Reflector
- dnSpy







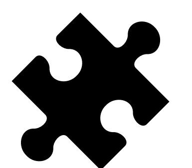
Против лома нет приема: защита

- Обфускация
- Подпись бинарника
- Упаковщики
- Полиморфные программы

Cons

- Не панацея
- Есть шанс сделать качество хуже



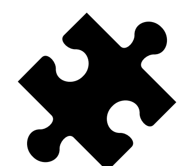


Кейс: не всегда дело в технике

- Windows старших серий
- Можно и без активации, но…

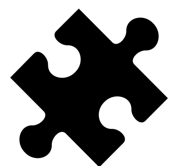






Кейс: не всегда дело в технике





Кейс: не всегда дело в технике

Позвоните и укажите свой код установки

Позвоните на один из этих номеров. Автоматическая телефонная система запросит ваш код установки (IID). В некоторых странах и регионах при звонках на бесплатные номера все же могут взиматься сборы.

Бесплатно:
(8) (800) 200 8002

Платно:
(7) (495) 745 5445 (Москва, Россия)

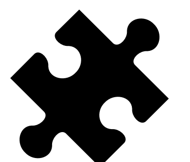
Код установки:

1	2	3	4	5	6	7	8	9
XXXXXXX	YYYYYYY	ZZZZZZZ	XXXXXXX	YYYYYYY	ZZZZZZZ	XXXXXXX	YYYYYYY	ZZZZZZZ

Прочтите заявление о конфиденциальности

Введите код подтверждения | Отмена





Кейс: не всегда дело в технике

- Думайте о всех ветках процесса
- Первым сорвут низковесящий фрукт
- Или даже выкопают картошку 🥔



И как дальше жить? Что делать?



- Отрицание, Гнев, …, Принятие
- Понять ваш пользовательский сегмент
- Выбирать модель защиты в зависимости от специфичных рисков



И как дальше жить в On premise?

- Привязка к железу
- Полуонлайн-активация
- Новая версия – новая лицензия
- Обфускация кода и навесная защита



И как дальше жить в Online?

- Тонкие клиенты решают все проблемы
- Но помните об AppSec и ошибках бизнес-логики
- Давно всем уже пора в браузер IMHO
- Но если это не про вас, то
  - Следите за количеством одновременно используемых инстансов
  - Анализируйте их поведение
  - Принимайте организационные меры



Artem @frydaykg Bachevsky



Обратная связь
и комментарии по докладу
по ссылке

